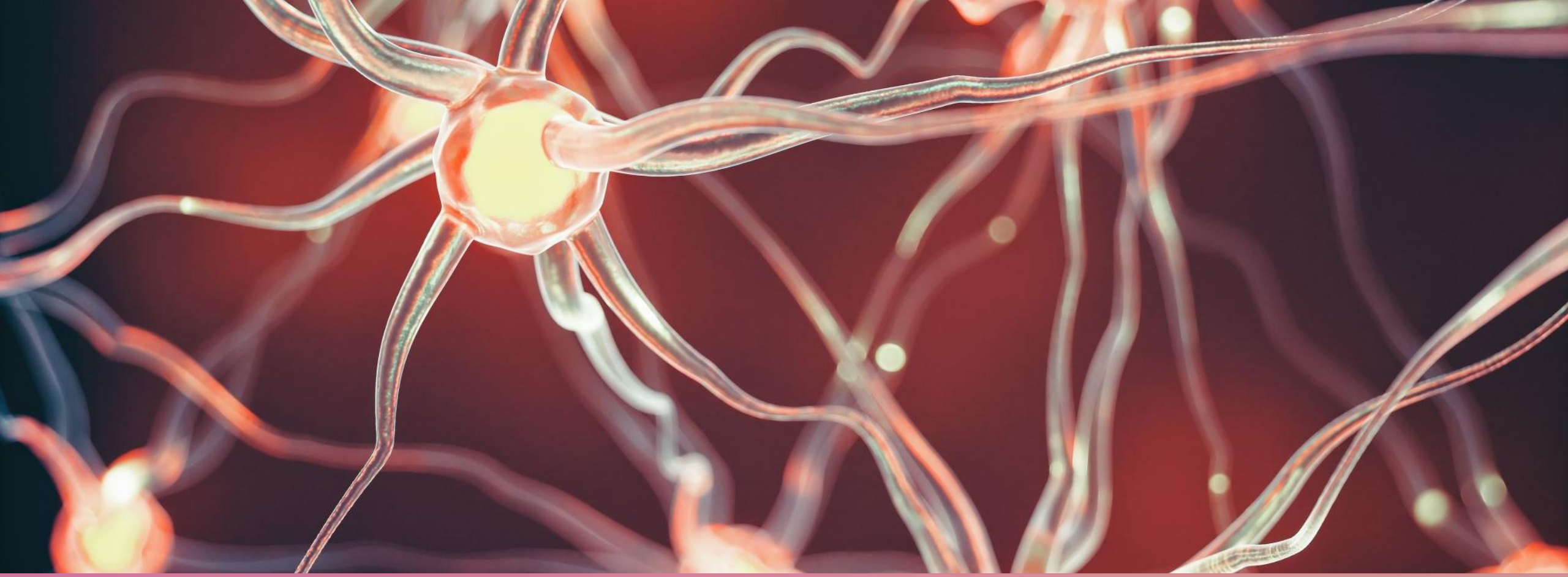
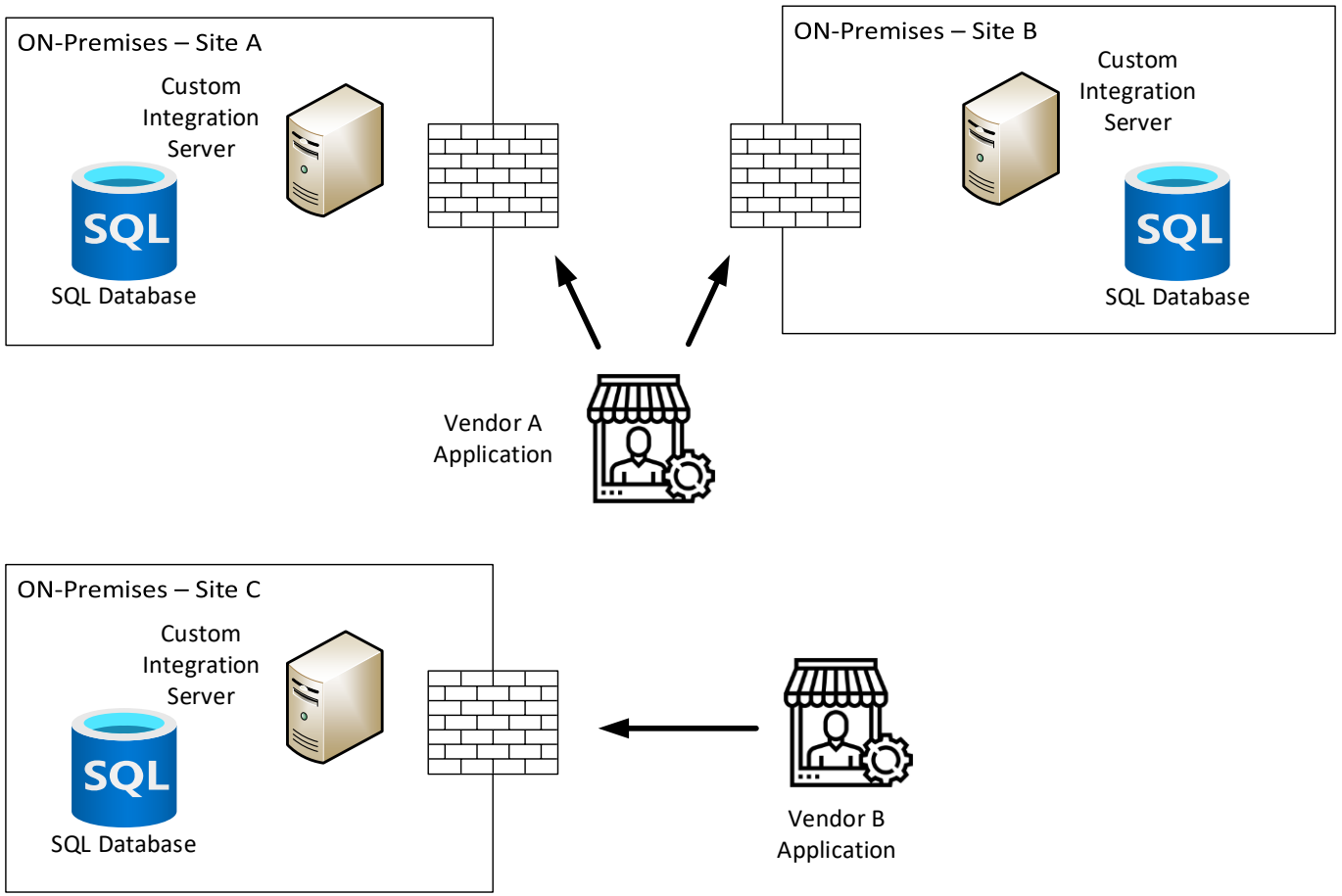


API SOLUTION OVERVIEW

FROM CONCEPT TO PRODUCTION

EXISTING SYSTEM

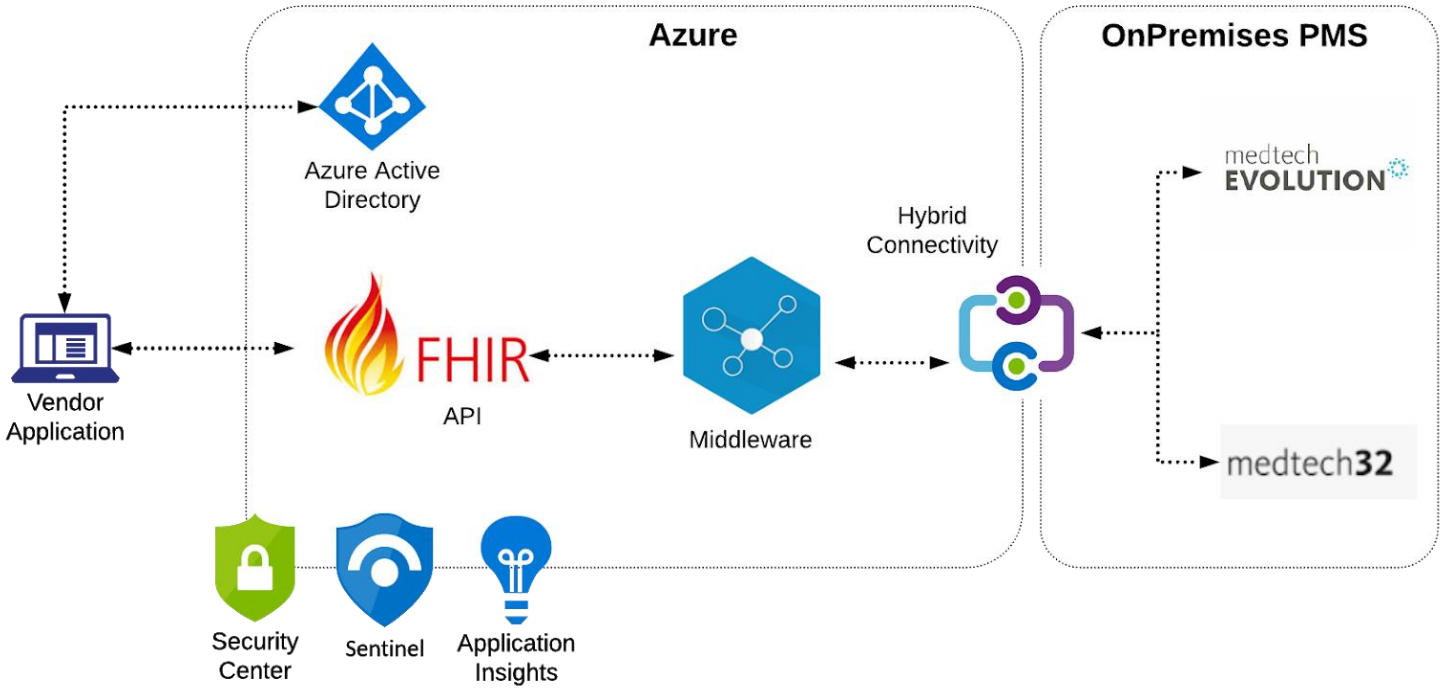


- Multiple Integrations
- Pin Holes
- Inconsistent Security models
- Management Overhead
- Complex
- Custom development
- Lack of Logging and Insights

DESIGN PRINCIPLES

- Data must remain On Premises
- No caching of any Personal Data
- Agile Approach
- API Response must be less than 8secs
- Cloud First Approach where possible
- Standards based approach
- No changes to existing on-premises services
- Automated Environment Builds

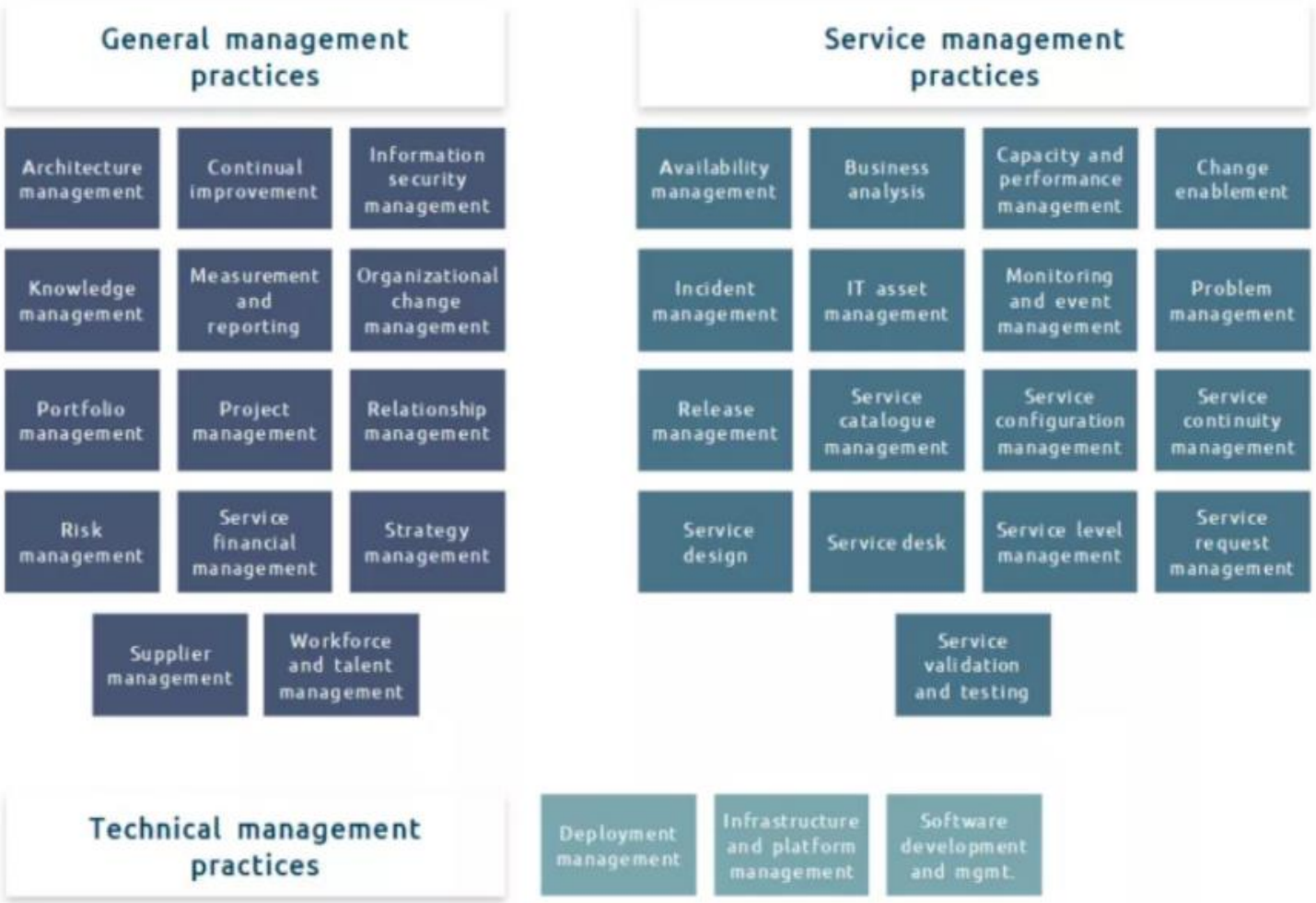
SOLUTION CONCEPT



Secure Consistent access for Vendor Applications while maintaining data silos

- Azure AD (who and what access)
- Microsoft FHIR Server – provides validation and authorisation
- Middleware – FHIR to DB Query Transformation and routing
- Hybrid Connectivity
- Azure Security Centre
- Azure Sentinel - Analyse Platform and Security Logs
- Application Insights monitoring end to end traffic flows

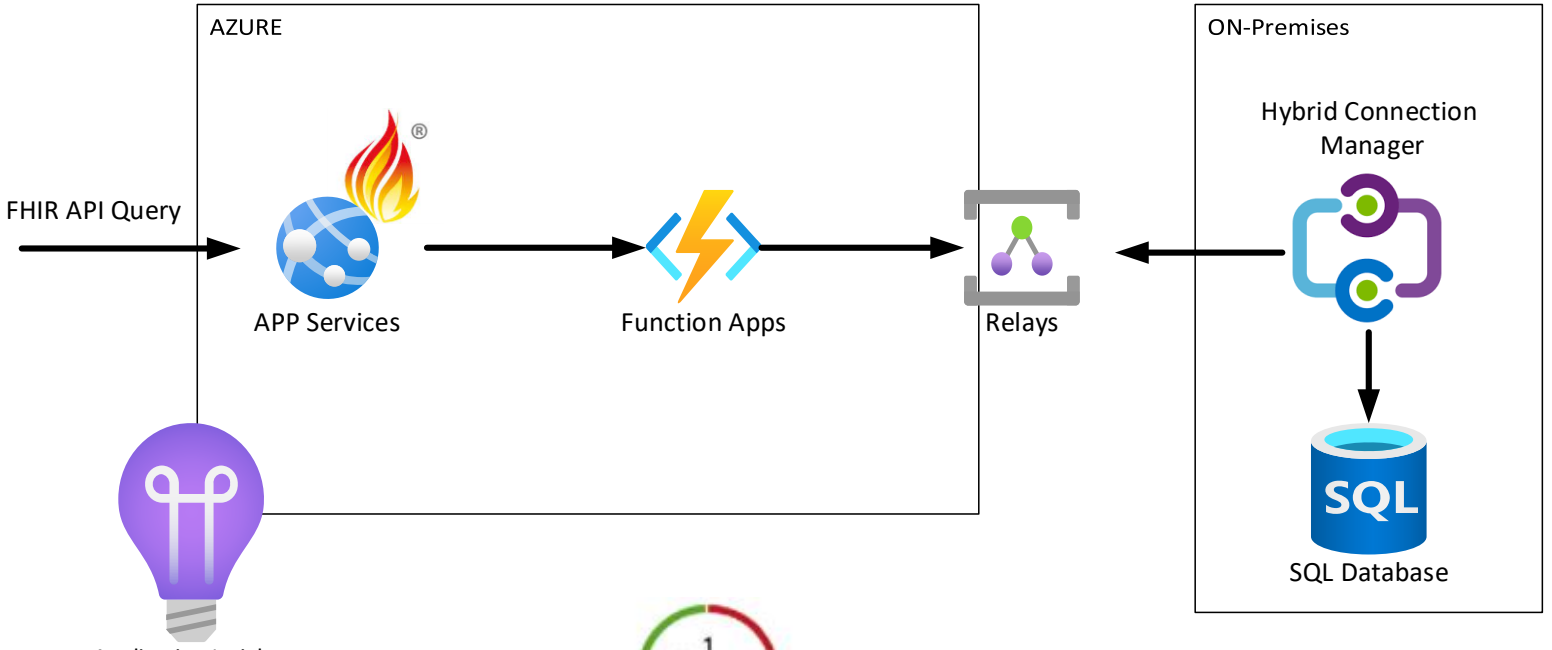
SOLUTION SERVICES



Managed Services

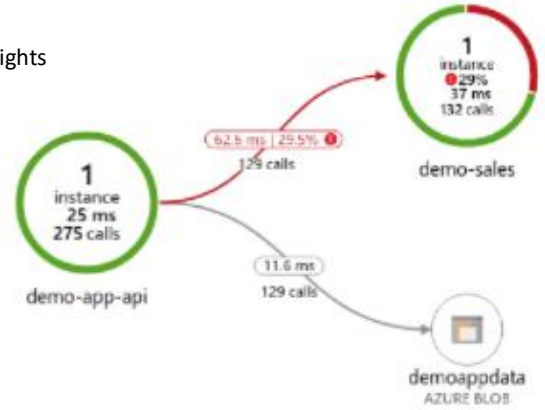
- Monitoring, troubleshooting, performance management
- Governance – Policy, Cost, Change Control, Architectural Guidance
- Technical Vendor Management
- DevOps Practice
- Vendor Onboarding
- Security Operations
- SLA and Reporting
- Service Desk

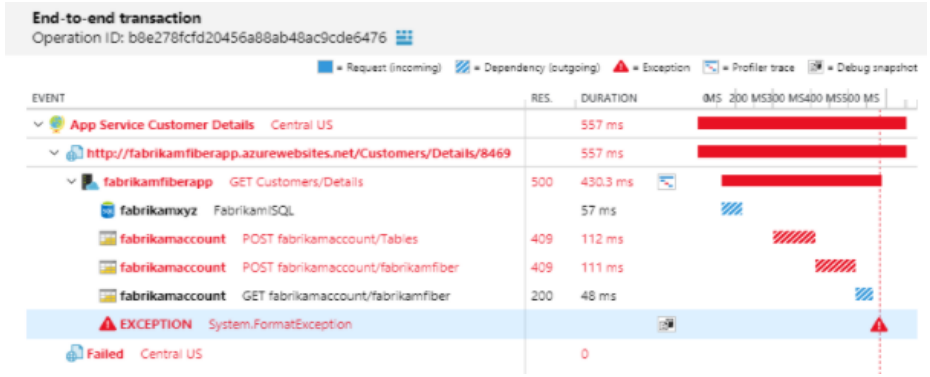
PROOF OF CONCEPT



Setup

- Modified Microsoft FHIR Server
- Reduced set of API Methods
- Single Relay to On Premises
- Single FHIR to SQL transformation Function App
- App Insights (end to end transaction trace)





DOCUMENTATION

High Level Project Plan

High Level Design

Detailed Technical Design

Work with Customer Timelines

Peer Review Microsoft / Aura

Onboarding User Guide

Testing Framework

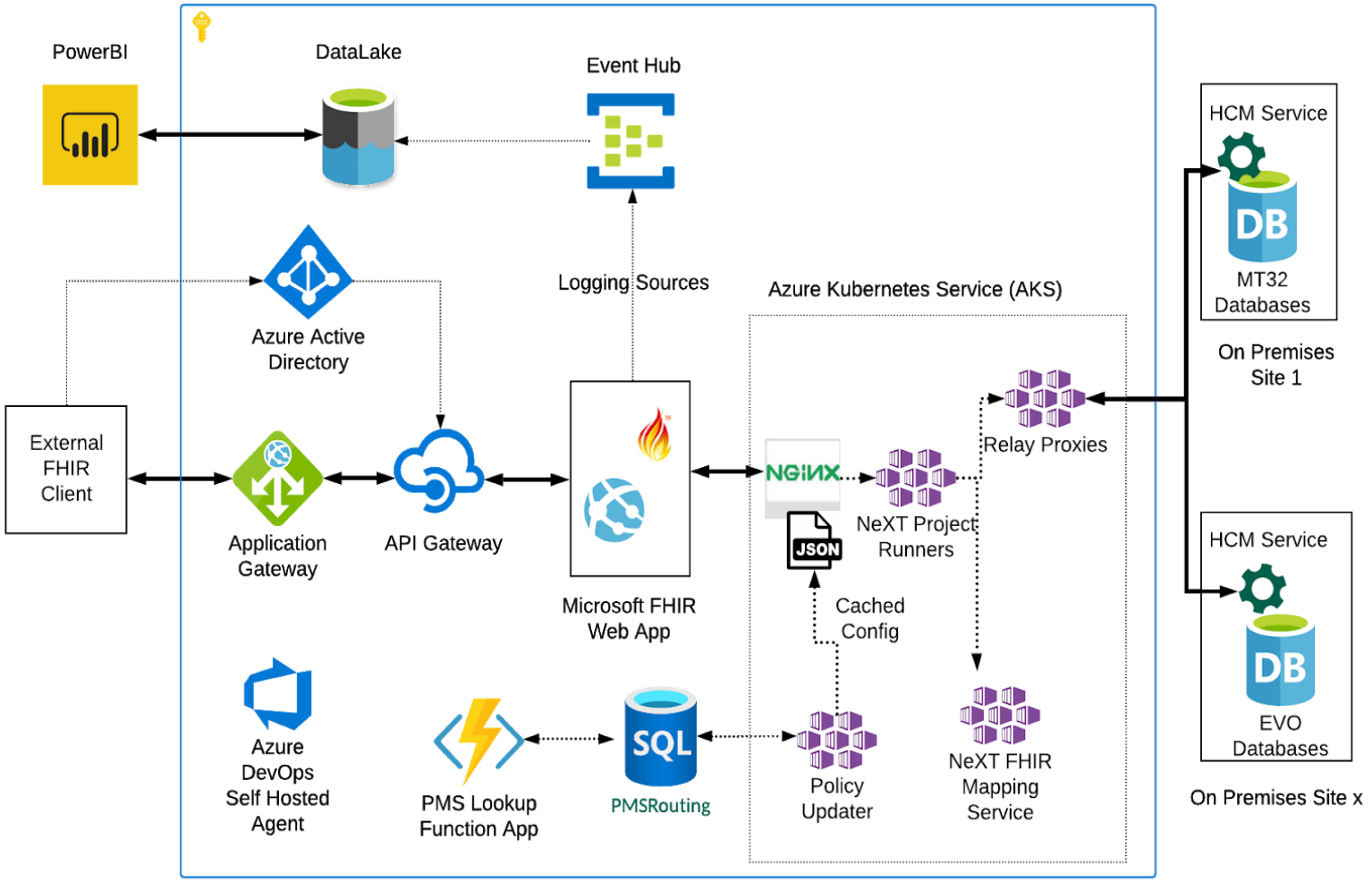
Other Documents to support future Feature Request Ideas and Road Map

Managed Service Design

Penetration Review

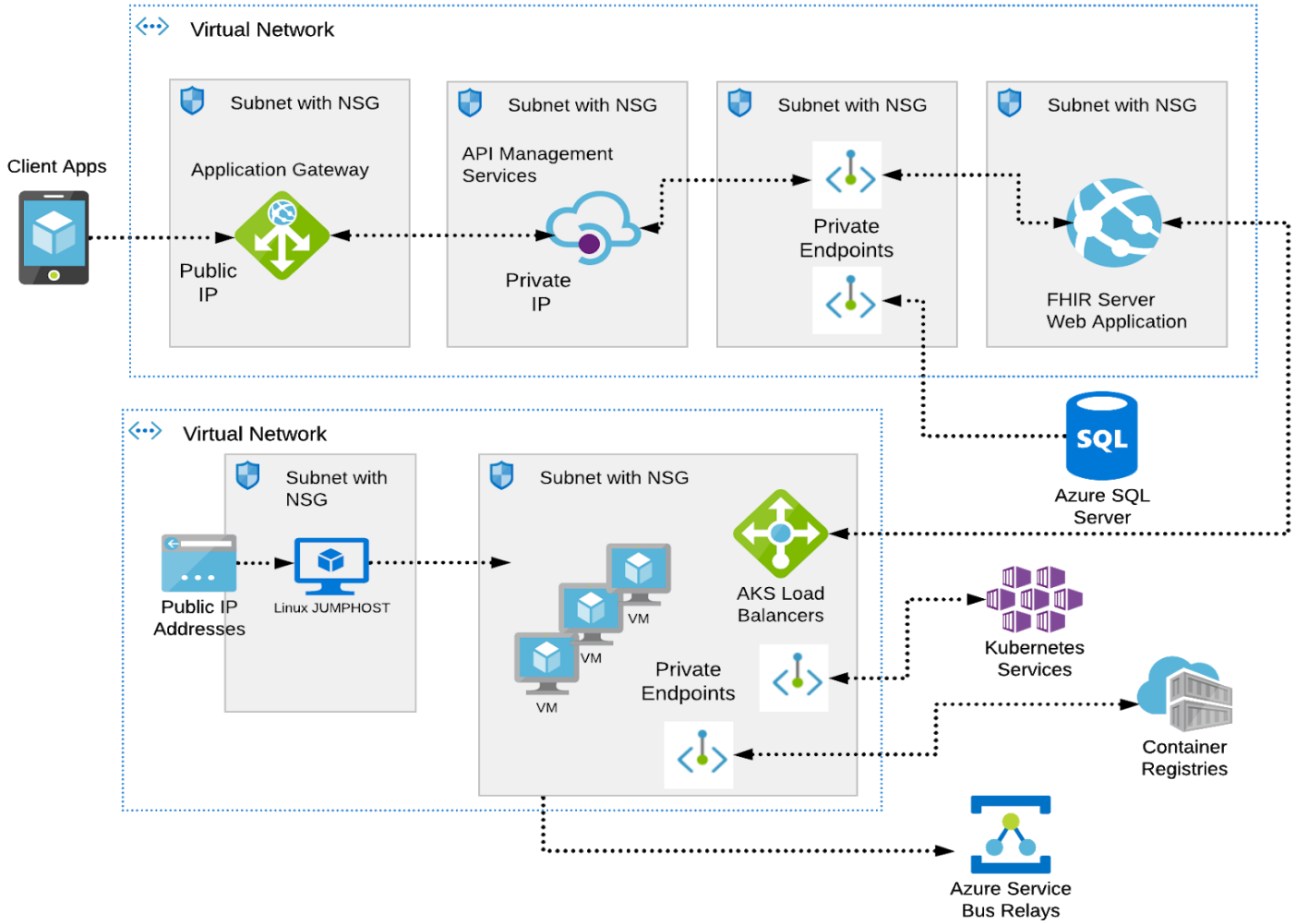
Azure Configuration Review

DETAILED DESIGN



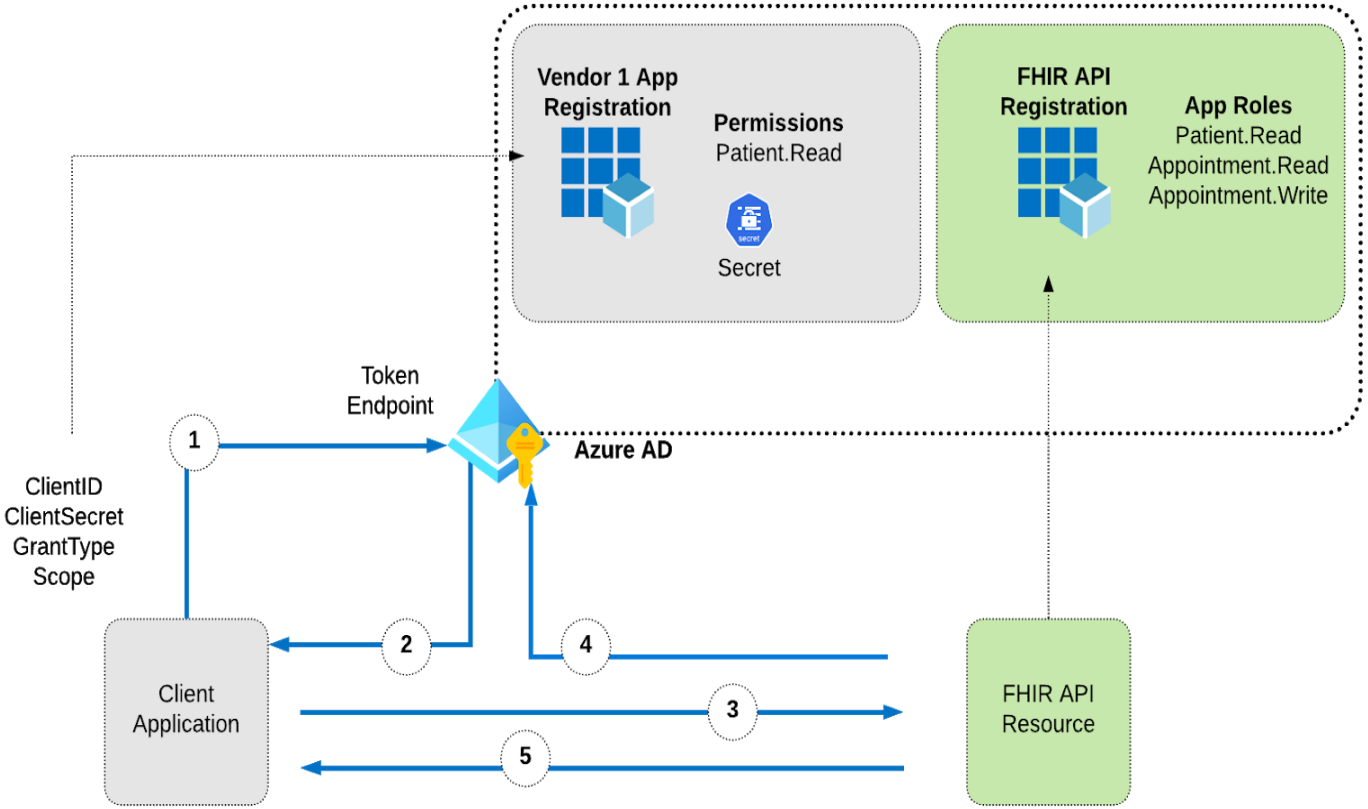
- Azure AD for Auth'n and Auth'z
- App Gateway and API Gateway for Message Routing
- FHIR Server - validation, enrichment
- AKS – middleware microservices
- Event Hub – API call logging for business
- SQL for configuration
- Hybrid Connectivity

NETWORK



- Virtual Network for FE and BE
- Subnets to isolate services
- Network Security Groups for Port level control
- Private Endpoints for natively Public services
- Management Subnet for Jump hosts
- Container Registry for Microservice Containers

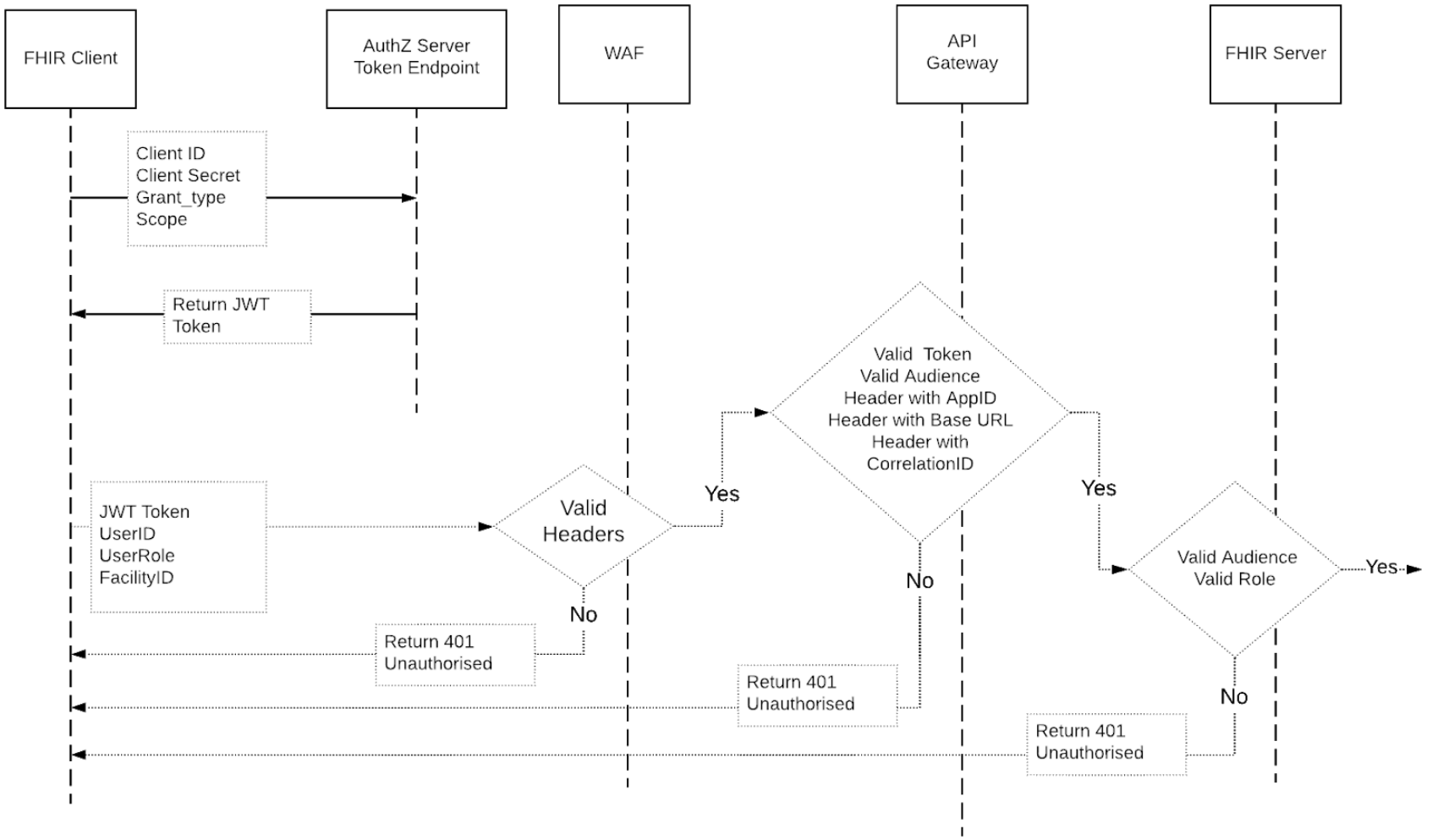
CLIENT CREDENTIALS



Azure AD App Registration

- Request to AD with credentials
- AD returns access token (JWT)
- API request contains JWT in Authorisation Header
- API Resource validates with AD the JWT
- If JWT contains correct permissions than response provided

JWT FLOW



High Level JWT usage

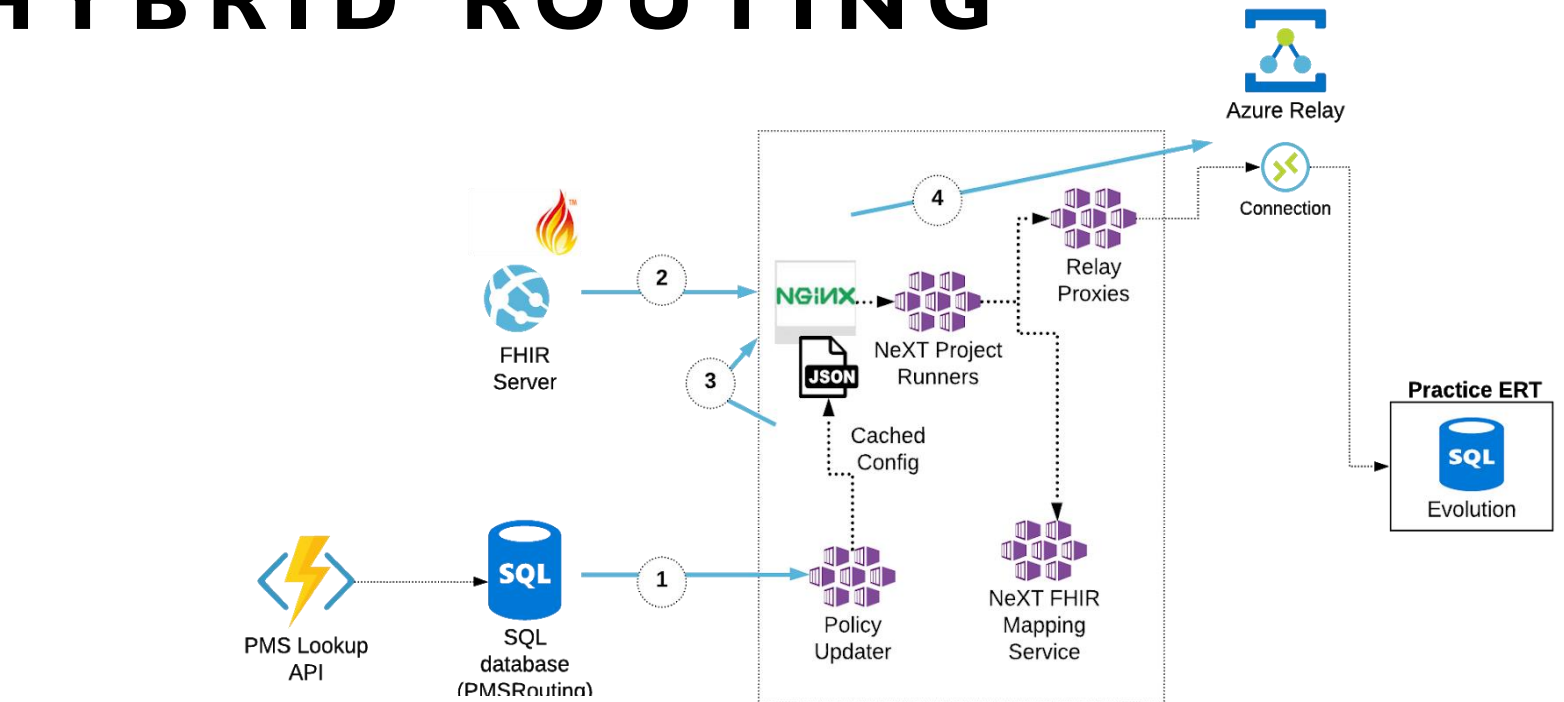
- AD Manages and distributes
- WAF validates request
- API Gateway validates issue
- FHIR Validates roles
- Easily extended to secure other APIs

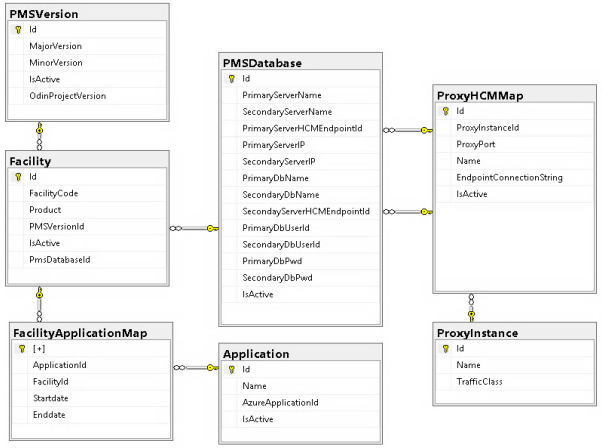
MESSAGE HYBRID ROUTING

High Level Routing

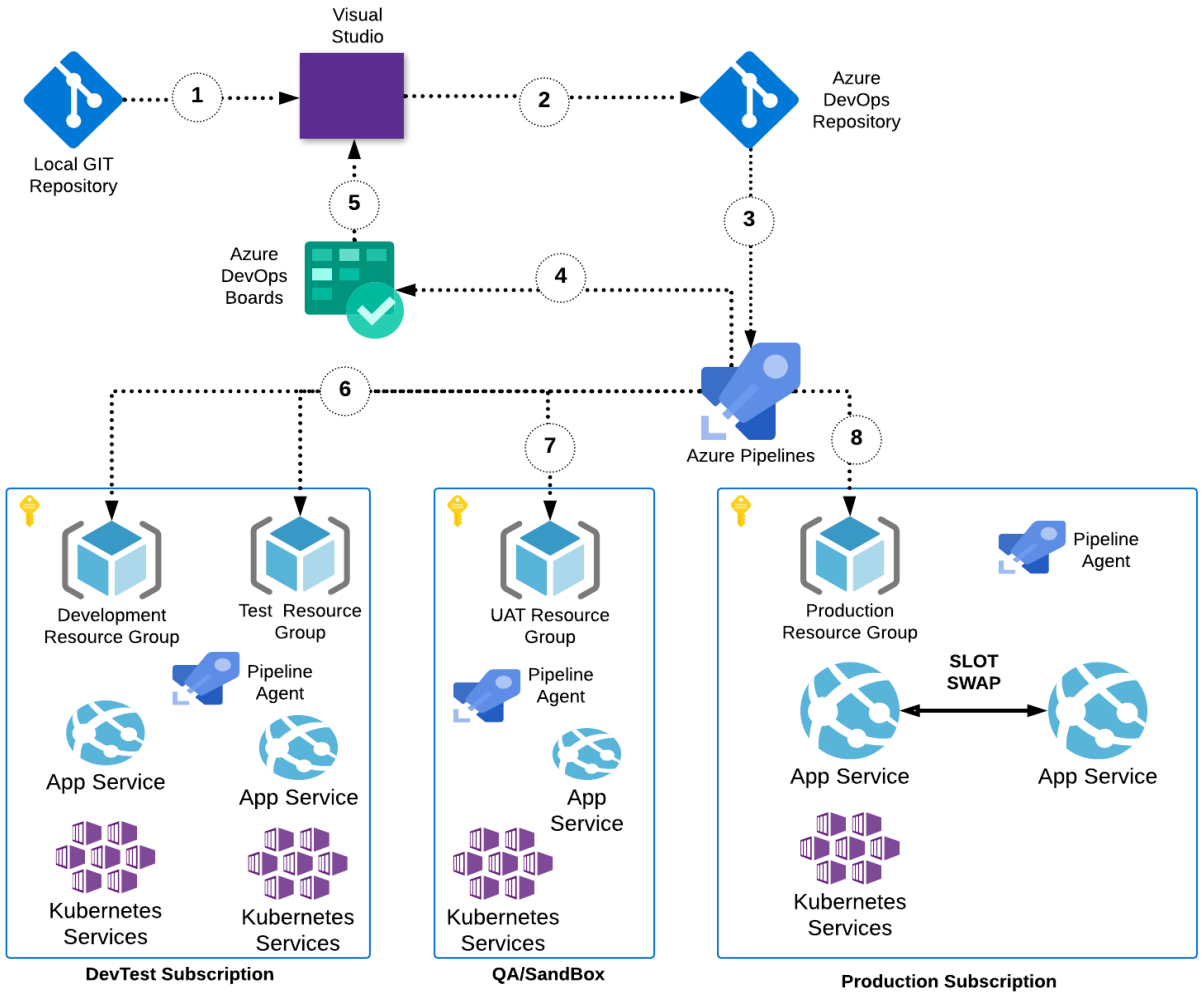
1. SQL Database stores mapping
2. Ingress POD receives Request
3. Cached Mappings Queried
4. Request routed to Relay EP

PMS API provided for a Web Application to manage and onboard new routes.





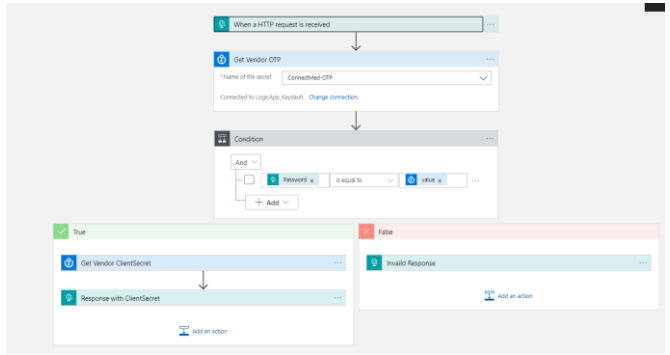
AZURE DEVOPS DESIGN



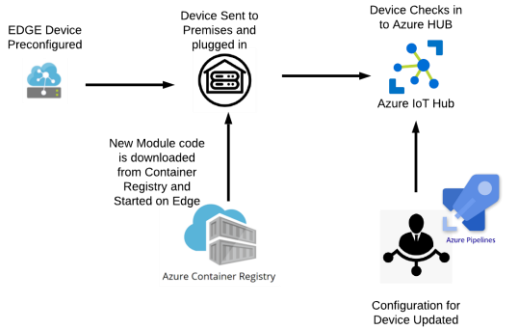
- Repository to store IaC, Application Code and Configuration
- Pipelines for different parts of the Solution
- Helm Charts for Kubernetes
- Agent in each environment
- Boards for managing – bugs, tasks, backlog..
- Landing Zone Tiered deployment for base Infrastructure

OTHER AREAS

- Use a Key Vault and Logic App to provide One Time access to the Client Credentials
  - URL Post with OTP and the Client Secret would be returned



- Provided a Concept around EDGE compute for each On Premises Locations
  - Using EDGE containers to manage access and SQL Platform



- Custom SLA Monitoring Solution (Can't use real Data)
  - Using DataDog
  - Create Mock API and data inside Kubernetes